RELATIONS BETWEEN ABSTRACT GROUP PROPERTIES AND SUBSTITUTION GROUPS.

By G. A. Miller.

It is customary to exhibit some of the fundamental relations existing between abstract groups and substitution groups by means of the following rectangular arrangement of the operators of the abstract group G:

$$\begin{array}{cccccc} 1 & s_2 & s_3 & \cdots & s_{g_1} \\ t_2 & s_2t_2 & s_3t_2 & \cdots & s_{g_1}t_2 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ t_\lambda & s_2t_\lambda & s_3t_\lambda & \cdots & s_{g_1}t_\lambda . \end{array} \qquad (A)$$

When the operators of the first row constitute a subgroup G_1 of G, the other rows are known as right co-sets of G with respect to G_1, and when all the operators of (A) are multiplied on the right by any operator of G, the rows of (A) are permuted as units according to a substitution on λ letters, which may be associated with the multiplying operator.

By using successively all the operators of G as multipliers there results a transitive substitution group K of degree λ which is isomorphic with G, and whose order is equal to that of G divided by the order of the largest invariant subgroup of G contained in G_1. In particular, a necessary and sufficient condition that K be simply isomorphic with G is that G_1 does not involve an invariant subgroup of G, besides the identity, and is not itself invariant under G, and a necessary and sufficient condition that K be a primitive substitution group is that G_1 is a maximal subgroup of G.*

The main object of the present article is to give a method for exhibiting fundamental relations between properties of an abstract group G and the subgroups of the isomorphic substitution group K which are separately composed of all the substitutions of K omitting one of its λ letters. Incidentally the following theorem relating to simply transitive primitive substitution groups is proved.

If in a transitive group of degree λ a subgroup composed of all its substitutions which omit a given letter has a transitive constituent of degree $\lambda - \alpha$, $\alpha > 1$, then for a fixed value of α only a finite number of values can be assigned to λ such that the transitive group of degree λ may be primitive.

The method noted in the preceding paragraph depends upon the known

* Cf. W. von Dyck, Mathematische Annalen, vol. 22 (1883), p. 90.

fact that, if we represent the λ rows of (A) by the letters $a_1, a_2, \cdots, a_\lambda$, then these rows are separately composed of all the operators of G which correspond to the substitutions of K which replace a_1 by a given letter. In particular, the first row of (A) is composed of all the operators of G which correspond to the subgroup of K composed of all the substitutions of K which omit a_1.

Suppose that G_1 is a non-invariant subgroup of G and that G_2 is one of the conjugates of G_1. It is known that each of the rows of (A) which involves at least one operator of G_2 must involve the same number of operators of G_2, and that at least one of the rows of (A) contains none of the operators of G_2.* When there is only one such row, it results from the fact noted in the preceding paragraph that the subgroup K_2 of K which corresponds to G_2 replaces one of the λ letters of K by $\lambda - 1$ letters, and hence this subgroup must be transitive and of degree $\lambda - 1$. That is,

A necessary and sufficient condition that K be multiply transitive is that the operators of G_2 appear in $\lambda - 1$ of the rows of (A).

When the operators of G_2 appear in exactly $\lambda - 2$ of the rows of (A), one of these rows besides the first involves operators which are found in each of the conjugates of G_2, since the number of these conjugates is $\lambda/2$. The operators of this row transform G_1 into itself and together with G_1 they constitute a subgroup H_1 of G. When G is represented in the form of a rectangle in which H_1 constitutes the first row, the operators of G_2 will appear in all except one of the rows of (A). A necessary and sufficient condition that H_1 be invariant under G is that $\lambda = 4$. When $\lambda > 4$, a conjugate of H_1 must involve G_2, and hence its operators must appear in all except one of these new rows. As these rows correspond to systems of imprimitivity of K the following theorem has been established:

If the operators of G_2 appear in $\lambda - 2$ of the rows of (A) then K has one and only one set of systems of imprimitivity and transforms these systems according to a multiply transitive group of degree $\lambda/2$.

From what precedes it results that when the operators of G_2 appear either in $\lambda - 1$ or in exactly $\lambda - 2$ of the rows of (A), then the same must be true as regards the operators of all the other conjugates of G_1 except those of G_1 itself. When the operators of G_2 appear in $\lambda - \alpha$ of the rows of (A), $\alpha > 2$, it is not necessarily true that the operators of the other conjugates of G_1, with the exception of G_1, appear in exactly $\lambda - \alpha$ of the rows of (A). This results directly from the fact that K_2 may then have transitive constituents of different degrees. A necessary and sufficient condition that one of these transitive constituents be of degree 2 is that all the operators of a conjugate of G_1 appear in exactly two rows of (A).

* Miller, Blichfeldt, Dickson, Finite Groups 1916, p. 68.

Whenever the operators of G_2 appear in exactly $\lambda - \alpha$, $\lambda > \alpha > 1$, of the rows of (A), the subgroup K_1 composed of all the substitutions of K which omit a given letter has a transitive constituent of degree $\lambda - \alpha$. When K_1 is transitive, then K has only one set of systems of imprimitivity such that each system involved α letters, and it permutes these systems according to a multiply transitive substitution group of degree λ/α, and all the conjugates of G_1, except G_1 itself, have operators in each of the same α rows of (A). When K has other systems of imprimitivity besides those involving α letters, these systems must involve a submultiple of α letters. In particular, when α is a prime number K has only one set of systems of imprimitivity.

When $\alpha > 2$ is a fixed number and K is primitive, K_1 must have a constituent of degree $\alpha - 1$. The subgroup of K_1 which corresponds to the identity of this constituent must be invariant under K_1, and if it is not the identity, it must appear in a conjugate of K_1 without being invariant under this conjugate.* Hence it must have a transitive constituent whose degree cannot exceed $\alpha - 1$. As the order of a substitution group of degree $\alpha - 1$ cannot exceed $(\alpha - 1)!$, the transitive constituent of degree $\lambda - \alpha$ contained in K_1 could not replace one of its letters by more than $(\alpha - 1) \cdot (\alpha - 1)!$ letters. It therefore results that when K is primitive $\lambda - \alpha \overline{\gtrless} (\alpha - 1) \cdot (\alpha - 1)!$ This constitutes a proof of the theorem noted above which may be stated as follows:

If the subgroup composed of all the substitutions of a transitive group of degree λ *which omit a given letter has a transitive constituent of degree* $\lambda - \alpha$ *then this transitive group is imprimitive whenever* $\lambda > (\alpha - 1) \cdot (\alpha - 1)! + \alpha$.

In the particular case when $\alpha = 3$ it follows from this theorem that K could not be primitive when $\lambda > 7$. As a matter of fact, it is easy to verify that in this special case K can only be primitive when it is the dihedral group of order 10 and of degree 5. When $\alpha = 4$ there are several possible primitive groups which satisfy the given conditions.

* G. A. Miller, Proceedings of the London Mathematical Society, vol. 28 (1896), p. 534.